Remarks

Reconsideration of this Application is respectfully requested. Claims 21, 22, 24-28 and 31-51 are pending in the application, of which claims 21, 31, and 43 are independent. By the foregoing Amendment, claims 21 and 24-28 are sought to be amended and claim 23 is sought to be cancelled without prejudice or disclaimer. Claims 31-51 are sought to be added. No new matter is embraced by this amendment and its entry is respectfully requested. Based on the above Amendment and the remarks set forth below, it is respectfully requested that the Examiner reconsider and withdraw all outstanding rejections.

Rejection under 35 U.S.C. § 103

The Examiner, on page 4 of the Final Office Action dated 12/10/08, states that claims 21-28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,973,577 to Kouznetsov and further in view of U.S. Patent No. 7,065,790 to Gryaznov. Applicants respectfully traverse this rejection. Based on the remarks set forth below, Applicants respectfully request that this rejection be reconsidered and withdrawn.

With respect to independent claim 21, the Examiner states that Kouznetsov substantially teaches Applicants' invention as recited in claim 21. Applicants respectfully disagree. Kouznetsov does not teach or suggest at least the elements of: "an execution area configured to perform operations to examine a set of instructions embodying an invoked application to identify the invoked application, obtain application-specific intrusion criteria, the application-specific intrusion criteria including intrusion signatures and behavior criteria, and monitor network communications for the invoked

application for application-specific intrusion signatures and abnormal application behavior to detect an intrusion."

Unlike the present invention, which "examine[s] a set of instructions embodying an invoked application to identify the invoked application", Kouznetsov, from the sections of Kouznetsov cited by the Examiner, teaches (1) that "[e]ach action is performed by one or more applications executing within a defined computing environment", Kouznetsov, column 2, lines 47-48, (2) that "[a] plurality of applications 33, 34, 35 are loaded into the RAM from storage devices 36 and executed by the CPU", Kouznetsov, column 4, lines 12-14, and (3) that:

> [a]lternatively, the histograms could be stored in a centralized database for analysis of distributed runtime state, such as described in the related, commonly-assigned U.S. Patent application, entitled "System and Method For Dynamically Detecting Computer Viruses Through Behavioral Analysis Of Distributed Runtime State Using An Analysis Tree," filed May 26, 2000, pending, the disclosure of which is incorporated herein by reference. The histograms are analyzed to identify repetitions of suspect behavior.
>
> FIG. 3 is a block diagram showing the functional software modules 50 of the monitor/analyzer 19 of FIG. 1. Each module is a computer program written as source code in a conventional programming language, such as the C or C++ programming languages, and is presented for execution by the CPU as object or byte code, as is known in the art. The various implementations of the source code and object and byte codes can be held on a computer-readable storage medium or embodied on a transmission medium in a carrier wave.

Kouznetsov, column 4, lines 28-47.

Thus, instead of "to examine a set of instructions embodying an invoked application to identify the invoked application," Kouznetsov teaches that actions are performed by one or more applications executing within a defined computing environment; a plurality of applications are loaded into RAM from storage devices and executed by the CPU; and that histograms are stored in a centralized database for analysis of distributed runtime

state. The remaining section of Kouznetsov identified by the Examiner to teach this element further teaches that the software modules of the monitor/analyzer are computer programs written as source code in a conventional programming language and are presented for execution by the CPU as object or byte code. See Kouznetsov, column 4, lines 37-47. Thus, none of the Examiner cited sections of Kouznetsov teach anything about Applicants' element "to examine a set of instructions embodying an invoked application to identify the invoked application."

The Examiner further states on page 4 of the Final Office Action dated 12/10/08, that Kouznetsov teaches Applicants' element of "an execution area configured to perform operations to ... obtain application-specific intrusion criteria". The Examiner states that Kouznetsov teaches this at column 2, lines 51-58, column 5, lines 9-12, and col. 7, lines 1-2. Applicants respectfully disagree. At column 2, lines 51-58, Kouznetsov teaches that:

> [t]he sequence of the execution of the monitored events is tracked for each of the applications. Each occurrence of a specific event sequence characteristic of computer virus behavior and the application that performed the specific event sequence, are identified. A histogram describing the specific event sequence occurrence for each of the applications is created. Repetitions of the histogram associated with at least one object are identified.

Thus, instead of "to perform operations to ... obtain application-specific intrusion criteria", as recited in independent claim 21, Kouznetsov teaches event sequence characteristics of computer virus behavior as the criteria, but the event sequence characteristics are not specific to any application and therefore, cannot be considered "application-specific intrusion criteria."

At column 5, lines 9-12, Kouznetsov discloses that "[t]he process identifier (ID) 71 and application name 72 fields respectively store the process number and name of the application 33, 34, 35 (shown in FIG. 2) to which the recorded monitored event is associated." Thus, instead of "to perform operations to ... obtain application-specific intrusion criteria", as recited in independent claim 21, Kouznetsov teaches storing the process number and name of the application to which the recorded monitored event is associated.

At column 7, lines 1-2, Kouznetsov discloses "records for the monitored events 70 are retrieved for each of the applications 33, 34, 35 (block 151)." Thus, instead of "to perform operations to ... obtain application-specific intrusion criteria", as recited in independent claim 21, Kouznetsov teaches retrieving the records for the monitored events for each application.

The Examiner further states on pages 4-5 of the Final Office Action dated 12/10/08, that Kouznetsov teaches Applicants' element of "an execution area configured to perform operations to ... monitor network communications for the invoked application for application-specific intrusion signatures and abnormal application behavior to detect an intrusion.". The Examiner states that Kouznetsov teaches this at column 2, lines 32-40 and column 4, lines 15-36. Applicants respectfully disagree.

At column 2, lines 32-40, Kouznetsov discloses a system and method for dynamically detecting computer virus activities by monitoring runtime execution states and comparing the runtime execution states to a set of monitored events. Subsequent events are tracked if a monitored event occurs. *Id.* Histograms are generated for

identified suspect sequence characteristics of potentially viral activity. *Id.* If the histograms illustrate repeated suspect sequences, a virus alert is generated. *Id.*

At column 4, lines 15-36, Kouznetsov further defines the monitoring of executing applications by a monitor/analyzer. System calls from the executing applications are compared to a list of monitored events. *Id.* If there is a match, it is determined whether the application is performing a sequence of suspicious actions characteristic of computer viruses, and if so, histograms are generated and stored. *Id.* The histograms are analyzed to identify repetitions of suspect behavior. *Id.*

Thus, unlike the present invention, Kouznetsov teaches monitoring the execution of applications for monitored events and if a sequence of these monitored events are occurring, then generating histograms and analyzing the histograms to identify possible computer viruses, not "monitor[ing] network communications for the invoked application for application-specific intrusion signatures and abnormal application behavior to detect an intrusion."

Thus for at least the above reasons, Kouznetsov does not teach or suggest Applicants' elements of: "an execution area configured to perform operations to examine a set of instructions embodying an invoked application to identify the invoked application, obtain application-specific intrusion criteria, the application-specific intrusion criteria including intrusion signatures and behavior criteria, and monitor network communications for the invoked application for application-specific intrusion signatures and abnormal application behavior to detect an intrusion."

The Examiner admits, and Applicants respectfully agree, that Kouznetsov does not clearly recite Applicants' element of "an execution area configured to perform

operations to examine a set of instructions embodying an invoked application to identify the invoked application". The Examiner further states that this element is taught by Gryaznov. Applicants respectfully disagree.

Gryaznov does not solve the deficiencies of Kouznetsov. Unlike the present invention, Gryaznov teaches receiving a sample of a computer malware and scanning the computer malware using anti-virus scanners to generate information identifying the computer malware. Thus, unlike the present invention, which is "to examine a set of instructions embodying an invoked application to identify the invoked application", Gryaznov is scanning samples of computer malware using anti-virus scanners to identify the computer malware.

The Examiner, on page 7 of the Final Office Action dated 12/10/08, states that Kouznetsov teaches Applicants' elements of: "applying a hash function to the set of instructions to generate a condensed representation" and "comparing the condensed representation with existing condensed representations for known applications," as recited in claim 28. Applicants respectfully disagree.

Kouznetsov does not teach or suggest at least the following element of "applying a hash function to the set of instructions to generate a condensed representation." In fact, Kouznetsov does not teach or suggest "a hash function" and, therefore, cannot teach "applying a hash function to the set of instructions to generate a condensed representation."

Thus, neither Kouznetsov nor Gryaznov, separately or in combination, teach or suggest Applicants' claimed invention as recited in independent claim 21 and dependent claim 28. For at least the reasons stated above, independent claim 21, and the claims that

depend therefrom (claims 22 and 24-28) are patentable over the cited references. Applicants respectfully request that the Examiner reconsider and withdraw the rejection of independent claim 21, and the claims that depend therefrom (claims 22, 24-28).

New Claims

New claims 31-51 have been added. Independent claims 31 and 43 include similar elements to independent claim 21. Thus, for at least the reasons stated above, independent claims 31 and 43, and the claims that depend therefrom (claims 32-42 and 44-51, respectively), are patentable over Kouznetsov and Gryaznov, separately or in combination.

Request for an Examiner Interview

Applicants respectfully request an Examiner Interview. Applicants respectfully request that the Examiner contact the Applicants' representative at the number provided to formally set a date and time to conduct the interview.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all currently outstanding rejections and that they be withdrawn. It is believed that a full and complete response has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Response is respectfully requested.

Respectfully submitted,

Intel Corporation

/Crystal D. Sayles, Reg. No. 44,318/
Crystal D. Sayles
Senior Attorney
Intel Corporation
(202) 588-1959

Dated: June 22, 2009

Intel Corporation
Customer Number 59796
c/o CPA Global
P.O. Box 52050
Minneapolis, MN 55402